⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭56—123066

⑤1Int. Cl.³	識別記号	庁内整理番号
G 06 F 15/30		7737—5B
15/00	102	6974—5B

⑬公開　昭和56年(1981) 9月26日

発明の数　1
審査請求　有

（全12頁）

⑤4取引実行システムのための個人認証方法

⑳特　願　昭56—3986
㉒出　願　昭56(1981) 1月16日
優先権主張　㉜1980年2月11日㉝米国(US)
㉛120222

⑦2発明者　ドナルド・ジョセフ・チエサレク
アメリカ合衆国カリフオルニア州ロス・ガトス・ベルブロッサム・ウエイ280番地
⑦1出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション
アメリカ合衆国10504ニューヨーク州アーモンク（番地なし）
⑦4代理人　弁理士　頓宮孝一　外1名

明　細　書

1. 発明の名称　取引実行システムのための個人認証方法

2. 特許請求の範囲

ホスト・プロセッサーに接続された端末装置を操作してカードから読取られたカード・データと鍵盤から入力された認証データとの関係を検査する取引実行システムのための個人認証方法にして、

前記カード・データ及び可変数を含む取引要求メッセージを前記ホスト・プロセッサーへ送信する段階と、

前記ホスト・プロセッサーにおいてファイルの認証データ検査欄を前記カード・データによつてアクセスする段階と、

前記アクセスされた認証データ検査欄と前記可変数とを結合し、その結果を暗号化する段階と、

前記暗号化の結果を含む取引応答メッセージを前記端末装置へ返送する段階と、

前記端末装置において前記取引応答メッセージにおける前記暗号化の結果を復号し、前記復号された認証データ検査欄と前記鍵盤から入力された認証データとを比較する段階と、

より成る取引実行システムのための個人認証方法。

3. 発明の詳細な説明

この発明は取引実行システムに関するものであり、特に、ホスト計算機が中央にデータ・ベースをもち、遠隔端末装置との通信によつて取引を実行するシステムを操作する方法に関する。例えば、これは特定の、ないし提携金融機関によつて発行された機械可読な暗証カードを入力すると同時に個人暗証番号を入力することに応答して、現金の払出しや金融機関同志の振替等を行うシステムであつて、この場合個人暗証番号は、暗証カード上のデータから得られるようになつていてもよいし、そうでなくてもよいものとする。

口座その他の情報を記憶した中央データベースをもつホスト計算機と端末装置が交信して現金の払出し等の取引を行う取引実行システムの存在は

広く知られている。このようなシステムの例としては、米国特許第３９５６６１５号、第３９７０９９２号、第３９３７９２５号、第４１８６８７１号さらに１９７９年２月２日出願の米国特許未決出願第００９３８４号がある。

端末装置を通じて現金の払出しや預金を行なうこのようなシステムは現代の熾烈なビジネス環境のもとで、銀行のサービス拡張のために広く用いられている。

この種の端末装置は通常、クレジット・カード上の情報を読み取る機構、鍵盤、表示機構、通帳出し入れ口を具えている。この端末装置は、データ・ベースと連係して操作することも、独立して用いることもできる。

銀行員を介さずに行われる現金の払出しや、その他の銀行取引における安全確保の向上は、各クレジット・カードに個人暗証番号（ＩＤ　Number）を与えることによつて保証される。クレジット・カードから読み取られた口座番号に対応する暗証番号が鍵盤から入力されたとき、はじめてクレジ

ット・カードによる取引が可能になる。

このような手続きを決めておけば、盗難ないし拾得カードによる端末装置からの現金引出し等を防止することができる。端末装置がデータ・ベースと連係して用いられる場合には、口座番号と暗証番号との対応性は自由に選ぶことができる。

しかし一方、暗証番号は、所定のコードに従つて口座番号から作り出すこともできる。

前者の場合については後に詳述する。

後者の場合は暗証番号を預金者が自由に選ぶことができるようにするため、カード上には口座番号と一緒に差引値（ｏｆｆｓｅｔ　ｖａｌｕｅ）を記録しておく。すなわちこの暗証番号は、所定のコードに従つて口座番号から作り出された番号とこの差引値が加え合わされるか或いは組み合わされた結果得られる番号が自由に選ばれた暗証番号に等しくなるように選ばれている。

このように暗証番号と、カード上の口座番号（および差引値）の間の関係を前もつて決めておけば、暗証番号と口座番号とを関係づける算法（ア

ルゴリズム）によつて、独立した（ホストと切り離された状態になつている）端末装置においても、暗証番号を検査することができる。

提携した複数の銀行が発行するクレジット・カードが同一の端末装置で使用される場合には、これらの銀行は、口座番号から暗証番号を作り出す際に、いずれも同一のコードないし算法を用いるか、これらの算法を区別する方策を提供しなければならない。

このようなシステムの一つとして暗証番号と口座番号との関係を決めるために、キー番号による算法を用いたものがある。このシステムにおいては、暗証番号と比較するための検査番号を生成するために、線形および非線形演算によつて、口座番号とキー番号が組み合わされる。前記米国特許第３９５６６１５号はこのようなシステムである。

しかしながら複数銀行が発行したカードを同一端末において用いられる場合には、すべての銀行は同一のキー番号を使わなくてはならず、また口座番号は、すべてのカード上で同一位置になくて

はならない。

この米国特許のシステムに対する一改良法は、各端末装置に、暗号化されたキーのテーブル（一覧表）を設けることである。このテーブルには、複数提携銀行が用いるキーによる算法、カード上の口座番号の位置（データ・トラック）を示すデータ、差引値その他、鍵盤から入力された暗証番号と比較される検査番号を生成するためのデータが記録される。

このシステムの改良型としては前述の米国特許第４１８６８７１号がある。これによればホスト計算機に「仮想金融機関テーブル（ＶＦＩＴ）」を設けている。利用者がクレジット・カードと暗証番号を入力すると、クレジット・カードにおいて指定された銀行に対応する項目を見付け出すために端末装置内の金融機関テーブル（ＦＩＴ）がまず探索される。もし目的の項目が見付かれば項目中のデータが用いられてクレジット・カード上の個人データが暗号化され、利用者が入力した暗証番号を検査するために用いられる。

もし端末装置のＦＩＴ中に目的の項目が見付からない場合はホスト計算機のＶＦＩＴの探索が行なわれる。ホストのＶＦＩＴ中に目的の項目が見付かるとそのデータは端末装置に送り返され、そこで暗証番号の検査が行なわれる。

別の方法としてはクレジット・カード上のデータと暗証番号をホストへ送つて、口座番号と暗証番号の検査（これをＰＩＮ検査という）を含む取引の認可をホストで行なうよう指示する制御ビットを、端末装置のＦＩＴ中に入れておくこともできる。

端末装置におけるＰＩＮ検査に加えてホストで行われるＰＩＮ検査については米国特許第３９５６６１５号に述べられている。このようなホストのＰＩＮ検査においては、端末装置から入力された暗証番号が２重に暗号化されて、カード上のデータと共にホストへ送られる。ホストにおいては、２重に暗号化された暗証番号は１重に復号され、暗号化されている暗証番号のデータ・ベースがカード・データによつてアクセスされる。データ・

ベースから取り出された暗号化されている暗証番号は、端末装置から受取つた「２重に暗号化されたものを１重に復号した」暗証番号と比較されてＰＩＮ検査が行なわれる。しかしながらこのシステムでは、もしホストにおけるＰＩＮ検査が通らなければ取引は認可（承認）されない。すなわちＰＩＮ検査は最初からやり直さなければならないことになる。

カード上のデータと鍵盤から入力された暗証番号の算法的関係に基づいたＰＩＮ検査が端末装置で行なわれる場合には番号が一致しないともういちど正しい番号を入力しなおすことになり、何回かやり直してもやはりうまく行かなければ取引が拒否される。

クレジット・カードと暗証番号に対し、テーブルとキーを使用する上述の検証方式によつて現金支払用端末装置の安全性は向上し、また複数銀行間が提携して他行カードによる現金の払出し等ができるようになつた。しかしこのシステムでは端末装置内に存在する大量の現金を入手したり、端

末装置から銀行間で口座への振替を行なつたりすることに不当に利用される弱点も残している。

重大な問題の一つに、端末装置が独立して働く場合にもオンラインで働く場合にも、端末装置における暗号化の算法に関する安全保護の問題がある。

現金支払用端末装置を連日稼動させるには多数の操作員や保守要員が必要になる。たとえば銀行の各支店には現金支払用端末装置の内部に接触できる行員が存在する。この人たちは通常の保守作業のために暗号キーに接することも間々あるでしろう。あるいは多少の訓練を受ければこの人たちが通信回線を盗聴したり、内部回路の電気的信号を測定したりすることにより、不当にキーを知りうることも考えられる。

いちど暗号化のキーを入手し、算法が判つてしまえば、膨大な数の口座番号と暗証番号の関連性を生成できることになる。さらにカードの様式、カード上の検証データや差引値の位置を知ることにより、カード・データと自由に選んだ暗証番号

との関連性を確認することもできる。

このことから提携関係にある銀行のいくつかは、カード・データと暗証番号とを関連づける暗号化キーを他行では知り得ないように、ＰＩＮ検査をそれぞれ自行のホストで行なうべきであると主張している。

しかし前述のとおり、この方法によれば、ホストにおけるＰＩＮ検査が通らないと取引を拒否しなければならない。利用者は最初の取引がＰＩＮ検査に合格せず拒否されたという表示があつたときには直ちに取引をやり直すことができる。しかしながらこの方法は利用者にとつてもシステムにとつても時間の浪費となり、経費の増大とシステム全体の可用性を低下させることになる。

発明の要約

この発明にかかわる取引実行システムは、検証（ｖａｌｉｄａｔｉｏｎ）番号を含む情報を記憶したデータ・ベースを含むホスト計算機を包含する。この検証番号は口座番号その他のデータを暗号化し

たものから作り出したものであつても、そうでなくてもよい。ホスト計算機には一つ以上の端末装置が連結され、各端末装置からは口座番号と暗証番号を入力する手段をもつものとする。

この発明においては、端末装置から入力された暗証番号は、第１の暗号キーを用いて暗号化され第１の結果を得る。第１の結果は端末装置で生成された変数と連結され、連結された番号は、さらに第２の暗号キーにより暗号化される。このようにして２重に暗号化された暗証番号が生成される。つぎに２重に暗号化された暗証番号は口座番号その他のデータと共にホストへ送られ、そこで２重に暗号化された番号は第２の暗号キーにより復号され第１の結果に戻される。そして第１の結果はホストのデータ・ベースにある、口座番号に付随する認証番号と比較される。

ホストにおいて認証番号と第１の結果とが不一致になつたが、取引自体は承認された、という場合には、ホストは認証番号と変数を連結して、これを第２の暗号キーによつて暗号化し、暗号化し

た認証番号を生成して、条件付きメッセージ中に入れ端末装置へ送り返す。

端末装置は条件付き取引承認メッセージ中の、暗号化された認証番号を復号して、比較のための認証番号を生成する。比較の相手は、再入力され第１のキーによつて暗号化された暗証番号である。この代替案としては生成された認証番号を第１のキーにより復号し、再入力された暗号化されない、ナマの暗証番号と比較する方法もある。

再入力された暗証番号と、条件付き取引承認メッセージ内のデータとの比較の結果、端末装置において取引が承認されることもあり得る。

発明の開示

この発明の内容、目的、利点を、より良く理解するために、参考として図、適用業務を付した説明およびこの発明における種々の新しい特長を以下に示す。

第１図に示すようにこの発明はホストＣＰＵ１０およびデータ・ベース１２を持つ銀行における

取引認可システムの改善に関する。

当業者には明らかであるが、ＣＰＵ１０は、たとえばＩＢＭシステム／３７０であつて、データ・ベースに対しＶＳＡＮ、ＩＳＡＭおよび／またはＳＡＭを通してアクセスし、ＤＯＳ／ＶＳ、ＯＳ／ＶＳ１、ＯＳ／ＶＳ２の元で働くＶＴＡＭ適用業務を実行するものと仮定してもよい。データ・ベース１２は、適用業務を処理するために必要なライブラリーおよび口座に関するファイルを持つている。後者には預金残高、入金・支払の記録等、口座に関する情報および後に詳述する認証番号が記憶されている。

また２つ以上の金融機関が提携し、相互のデータ処理システムを結合している場合も考えられる。これはＣＰＵ１０および１６を結ぶ線１４で示されている。

ＣＰＵ１６は、客先の口座データ等を記憶するデータ・ベース１８に接続されている。

Ｂ銀行のＣＰＵ１０は通信ループ３６を通して複数の銀行端末装置２０、２２が接続されている。

これはＳＤＬＣ網（ここには図示されていないが）を通して直接に接続されていてもよいし、たとえばＩＢＭ３６１０金融機関通信制御装置２４を通して接続されていてもよい。線２６は、たとえばＣＰＵ１０のＶＴＡＭによつて制御される通信回線およびＮＣＰ／３（回線網制御プログラム第３版）によつて制御されるＩＢＭ３７０４／３７０５通信制御装置を含むことを示す。制御装置２４はデータ・ベース１２に含まれるデータの一部である口座データを記憶するために、ディスケットを装備している場合もある。

Ｂ銀行のＣＰＵ１０には端末装置２０、２２が接続されていることが示されているが、同様にＡ銀行のＣＰＵ１６も所要の数の銀行用端末を備えているのが普通である。このような場合には提携銀行は、利用者がどこの銀行の端末から取引を行なつてもよいことを認めている。

この場合、Ａ銀行の発行した機械可読な認証カードの所有者がＡ銀行の端末装置２０に付属するキュッシュ・ディスペンサー２８を通じて自分の

口座から現金を引出したり、あるいは預金、振替、残高等の問合せ、払込み等、何らかの取引を行いたいと考えたとする。

利用者が端末装置２０を使用して取引を行なうことができるようにするためには、通常まず機械可読な口座カード（認証カードないしクレジット・カード）を機械に挿入し、鍵盤から個人認証番号（ＰＩＮ）を入力する。口座カードから読み取られたデータにはＰＩＮの正当性を検査するための、口座番号の全部または一部が含まれている。この正当性検査すなわちＰＩＮ検査はつぎのようにして行なわれる。

まず、カード・データかＰＩＮのいずれか一方を暗号化し他方と比較する。すなわち暗号化されたカード・データをＰＩＮと比較するか、暗号化されたＰＩＮをカード・データと比較するか、である。この暗号化はキー番号の制御の元で行なわれるが、これについては米国特許第３９５６６１５号および同第４１８６８７１号に詳述されている。後者には金融機関テーブル（ＦＩＴ）の存在

が述べられている。これによれば、Ａ銀行から発行されたカードを、端末装置２０で検査するために、端末装置２０の記憶機構内にＡ銀行の暗号キーを記憶できるように考案している。しかしながらＡ銀行はＢ銀行との提携には同意したものの、ＣＰＵ１０、制御装置２４、および／または端末装置２０、２２に記憶されるＡ銀行のＦＩＴ中に暗号キーを入れたくないという状況もありうる。さらにＡ銀行は、口座カード上のコード化されたデータから生成されないＰＩＮを利用者へ発行することもありうる。いずれの場合も端末装置２０は読取装置３０によつて読み取られた口座カードと、鍵盤３２から入力されたＰＩＮとの一致性を検査することはできない。

この状況においては、利用者は表示装置３４等を通して、取引に必要なもつと詳しい情報を入力するよう要請されることになる。この点については米国特許第３９５６６１５号および第４１８６８７１号さらに同未決出願第００９３８４号に詳述されている。ホストにおいて行なわれるＰＩＮ

検査に必要なこの情報（これには口座認証の情報も含まれる）はカード読取装置３０で読み取られるか、鍵盤３２から入力されるかして、ＰＩＮ検査のためホストすなわちこの場合はＣＰＵ１６へ送られる。これについては後に詳述する。これはＢ銀行についても同様であつて、口座カード上に記録されたデータから生成されないＰＩＮをＢ銀行が発行した場合、端末装置２０、２２に対しＢ銀行の利用者から受取つたデータを制御装置２４またはＣＰＵ１０へ、ホストＰＩＮ検査のために送るよう要求することもありうる。

第２図を参照すると、この例では代表的な取引を行なうための端末装置２０とホスト（制御装置２４もしくはＣＰＵ１０）間の通信が、要求メッセージ４０、取引応答メッセージ４２、状況メッセージ４４を含む３メッセージ・プロトコルに従つて行なわれる。（これは米国特許第４１８６８７１号に第５図と関連しておよび米国特許未決出願第９３８４号に第１２図と関連してＶＦＩＴおよび取引を処理する対話式の関連メッセージにつ

いて詳述されている。）第３図を参照すると、この例ではＢ銀行の端末装置２０からの通信が、同じメッセージ・プロトコルに従つてＢ銀行からＡ銀行のホスト１６へ送られる例が示されている。この場合にも上述のＶＦＩＴと対話メッセージが含まれうる。適用業務プログラムによつては、通信時間の短縮、記憶装置の節約、端末装置の利用度向上の目的で、取引の処理が、ホストを構成する２４、１０、１６等の装置において分散して行なわれることもある。

第４図を参照して、ここではホストにおいて安全かつ最適の初期ＰＩＮ検査を実施するために端末装置２０が取引要求メッセージ４０を生成する操作について記述する。

これはＰＩＮがＩＤカード上のデータから生成されない場合、あるいはＰＩＮとカード・データとの対応を検査するための暗号キーが端末装置に入つていない場合、さらには端末装置で行なわれたＰＩＮ検査が合格せず、ホストに送られてさらに検査が行われる場合等に必要になる。

上述のいずれかの状況下で、ホストにおける初期ＰＩＮ検査に不合格となつた場合には、引続き端末装置において再度入力されたＰＩＮに基づき検査が行なわれる。これによつてＰＩＮ検査のため再度ホストとの通信をやり直さずに済み、口座カードに対応する正しいＰＩＮの盗聴による漏洩を防ぐことができる。

端末装置２０はプログラム式のマイクロ・プロセッサーを備えており、マイクロプログラムの制御の元で働く。これに関しては米国特許第３９５６６１５号および同第４１８６８７１号に詳述されている。

ＩＤカード３８はカード読取装置３０によつて読み取られ、金融機関認証データを発生する。このデータは金融機関テーブル（ＦＩＴ）４６をアクセスするのに使用される。ＦＩＴ４６中のデータはＡキーの制御の元で復号され、ＰＩＮキー５０を生成する。このキーは金融機関ごとに個別に（一意に）決められているものである。

復号の段階４８およびその他すべての暗号化／

復号の過程は合衆国政府標準局の発行による「計算機データ保護のための暗号算法」連邦登録Ｖｏｌ．４０、Ｎｏ５２、１９７５年３月１７日（月）１２１３４～１２１３８ページに示されたもの〔以下これをＤＥＳ（Ｄａｔａ Ｅｎｃｒｉｐｔｉｏｎ Ｓｔａｎｄａｒｄ）と略す〕による。当業者には明らかであるが、ＤＥＳはハードウエアの一部によつて構成されていてもよいし、マイクロコードであつてもよい。

ＦＩＴ４６からは当該金融機関のためのＰＡＤ数字５２が得られる。これは利用者が鍵盤３２から入力したＰＩＮ５４の数字と連結されて６４ビットの番号を生成し、ＰＩＮキー５０の制御の元で段階５６においてＤＥＳにより暗号化される。暗号化されたＰＩＮ＋ＰＡＤ５８は６４ビットから成り、そのうち５６ビットは変数生成機構６０によつて生成された変数からの８ビットと連結される。このようにして連結された番号６２は、通信キーすなわちＣキーの制御の元でＤＥＳにより暗号化される。

変数生成機構は、たとえば取引一連番号や紙幣

計算機構の番号など、何らかの取引や、端末装置に関連して算法的に一つの番号を生成する。Ｃキーは通信キーであつて、端末装置とホスト・システム間の通信リンクにおけるデータの安全保護に使用される。

暗号化段階６４の出力は６４ビットの、２重に暗号化された番号であり、暗号化されたＰＩＮ＋ＰＡＤ５８の残りの８ビットと連結されて、７２ビットの暗号化された認証番号６６を形成する。これは取引要求メッセージ４０のうちの暗号化された部分である。暗号化されない情報７０には、たとえばホストが取引要求を処理するさいに必要なデータ、すなわちカード３８から読み取られたデータあるいは鍵盤３２から入力された取引の種類、金額（ただしＰＩＮは含まれない）等がある。ヘッダー７２にはメッセージの種類および端末装置のアドレスが含まれている。第５図を参照して、ホストであるＡ銀行およびＢ銀行においてＰＩＮ検査が行なわれ、取引応答メッセージ４２が生成される過程を以下に示す。

Ｂ銀行を例にとると、取引要求メッセージ４０には、その暗号化されない情報部分７０にデータ・ベースをアクセスするための番号が含まれている。この番号はＩＤカード３８から読みとられた利用者口座番号に関連する。

段階７４において、データ・ベースをアクセスするための番号が要求メッセージ４０から読み取られアドレスまたは探索引き数として認証データを取り出すのに用いられる。認証データはＰＡＤと連結されて暗号化された利用者ＰＩＮであつて、暗号化されたＰＩＮ＋ＰＡＤとしてデータ・ベース１２に記憶されている。

このように利用者ＰＩＮはホスト・データ・ベース中に、判然とした形（ナマの形）で記憶されているわけではないので、承認された要員以外の人が読んでも判らないようになつている。

段階７６においては第６図に関連して後に詳述するが、取引要求メッセージ上の暗号化されたデータ６８が復号される。

段階７８においては取引承認の処理で始まり、

ホスト銀行の適用業務プログラムによつて定められている、口座残高、入金・支払の記録、紛失・盗難カードの検査などが行なわれる。

上述の検査により取引が承認されなければ、段階８０においてホスト１０は取引応答メッセージ４２を作り、段階８２において、端末装置２０に対し通信による取引を拒否する。

取引が承認された場合には段階７８の口座検査に基づき、段階８４において、少くとも取引応答メッセージ４２の基本部分が作られる。これは前述の米国特許中に詳述されている。

段階８６においてはホストＰＩＮ検査が行なわれる。この検査は、第４図の段階７４においてデータ・ベース１２から得られる、暗号化されたＰＩＮ＋ＰＡＤ欄と、第５図の段階７６において取引要求メッセージから得られるＰＩＮ＋ＰＡＤの欄とが比較されて行なわれる。

もしホストＰＩＮ検査が合格すれば、段階８４において取引応答メッセージ４２が生成され、段階８２において取引の承認が端末装置２０へ送ら

れる。もしホストＰＩＮ検査が不合格になれば、段階８８において、条件付き承認を示す取引応答メッセージが生成され段階８２において端末装置２０へ送られる。

段階８０または８４において生成された、承認または拒否を示す取引応答メッセージの様式は第８図のとおりである。

段階８４および８８において生成された取引応答メッセージを第１１図に示す。このメッセージは条件付き取引承認であることを示し、同時に端末装置内において条件付き取引承認の状況を確立する。

段階８８においては応答メッセージ４２の中の、ＰＩＮ検査を要請するビットによつて、暗号化された暗証データ欄９０が生成される。これは第７図と関連して後述する。

条件付き承認応答メッセージにおいて、端末装置側では再度ホストとの連結を確立し直すことなく、利用者が正しいＰＩＮを再入力することができるようになる。

第６図を参照する。以下は取引要求メッセージ４０の暗号化された欄６８から暗号化されたＰＩＮ＋ＰＡＤをホストが生成する過程である。段階９２においては、暗号化された欄６８が、通信キーＣを用いて復号される。結果としての６４ビットには、変数生成機構６０（第４図）からのデータを表わす８ビットの部分が含まれ、また欄６８のうち残りの８ビットと連結される５６ビットが含まれる。これは暗号化されたＰＩＮ＋ＰＡＤ９４となり、第４図におけるデータ５８に等しく、段階８６においてホストＰＩＮ検査に用いられる（第５図）。

第７図を参照する。段階８８（第５図）において、条件付き承認を示す取引応答メッセージ４２のために、暗号化されたデータ・ベース中の認証番号９０を、ホストＣＰＵ１０が生成する過程を以下に示す。この方法によればＰＩＮ認証データの要素（この例ではデータ・ベース中のＰＩＮ＋ＰＡＤ）は、通信回線に乗らない。したがつて盗聴されることはないから、端末装置２０を操作し

て現金を不正に払出されるおそれもない。

変数生成機構においては以下のいずれを行つてもよい。第１の方法では、変数は変数生成機構により単純に生成されたものであつてもよい。これは段階９２において復号の出力として用いられる（第６図）。第２の方法は乱数を用いるものである。第３の方法としては、たとえば取引要求メッセージ中のある量（たとえば取引一連番号など）から算法的に生成してもよい。変数生成機構９６からの出力である８ビットは、データ・ベース１２から得られた６４ビットの暗号化されたＰＩＮ＋ＰＡＤのうちの５６ビットと連結されそして段階９８において通信キーＣを用いてＤＥＳにより暗号化される。この結果としての６４ビットは、データ・ベース１２からの、暗号化されたＰＩＮ＋ＰＡＤの残りの８ビットと連結されて、取引応答メッセージのために、７２ビットの２重に暗号化された欄を作り出す。

第９図を参照して、取引応答メッセージ４２を受け取つた端末装置２０によつて行なわれる処理

過程を示す。段階１００において応答メッセージの基本部分中の選ばれた欄に対して基本的な認証検査が行なわれる。もしこの検査の結果、取引が承認されないと決まつたときには段階１０２において取引は終了し、段階１０４において取引状況メッセージがホスト１０へ送られる。

もし取引が無条件に承認されれば、端末装置２０が、段階１０６において取引を完了し、状況メッセージを送り返す。

もし取引が条件付きで承認されたときには、利用者は新しいＰＩＮを１度ないし数度入力でき、そのＰＩＮとデータ・ベースに記憶されていた暗号化されているＰＩＮ＋ＫＥＹとの対応性が端末装置２０において検査されることになる。場合によつてはさらに用心のために変数の検査が付け加えられることもある。

段階１０８においては、第１０図に示された手順に従つて暗号化された認証データ９０が復号される。段階１１０においては変数生成機構によりホスト側で生成された変数欄が、端末装置２０に

よつて事前に（または再び）生成された変数と比較検査される。この検査は、もし変数生成機構が乱数を生成する場合には行なわれない。もしこの付加的な変数検査が合格しなかつた場合には、取引は中止される。

段階１１２において利用者はＰＩＮを鍵盤３２から入力するよう指示される。この、新たに入力されたＰＩＮは最初に入力されたもの（第４図におけるＰＩＮ５４）とは異なるものになるであろう。これは利用者が正しいＰＩＮを忘れて、もういちど打鍵するような場合に行なわれる。段階１１４において新たに入力されたＰＩＮは、ホスト・データ・ベースからのＰＩＮと比較され、その結果が等しければ取引承認状況となり、段階１０６における取引が可能となる。もし等しくなければ、何回か決められた回数だけ入力が繰り返され取引が終了する。段階１１４の比較の準備において暗号化されたデータ９０は、第１０図に示された手順に従つて２重に復号される。あるいは新たに入力されたＰＩＮは、第４図、段階５６の手順

に従つて暗号化することもでき、認証データ９０は第１０図、段階１１６の手順により１回復号される。

第１０図を参照する。ここでは端末装置２０において行なわれる処理過程を記述する。

ここでは段階１１４（第９図）において、新たに入力されたＰＩＮと、データ・ベース１２へ記憶するために暗号化されたＰＩＮを比較する検査の準備として、すでに暗号化されている認証欄９０を２重に復号する。まず、段階１１６においては通信キーＣが用いられＤＥＳによつて認証欄９０の７２ビット中の６４ビットが復号される。結果としての６４ビットのうち５６ビットは認証欄９０の残りの８ビットと共に、１重に復号された（すなわち１重に暗号化された）ＰＩＮ＋ＰＡＤ１１８を形成する。復号の段階１１６の結果としての６４ビット中、残りの８ビットはホスト１０において、変数生成機構により生成された変数であり、第９図の段階１１０における検査に用いられる。１重に暗号化されたＰＩＮ＋ＰＡＤはホス

トのデータ・ベース１２に記憶されているものと同じ番号である。段階１２０において、こんどはＰＩＮキー５０を用いてこれは再度ＤＥＳにより復号され、新たに入力されたＰＩＮと比較できるよう完全に復号されたＰＩＮ番号を作り出す。

本発明を実施する最善の方法

第１図および第２図に関連し、以下、この発明による取引実行システムの動作を説明する。端末装置２０において、取引要求メッセージ４０が生成される。このメッセージ中には鍵盤３２から入力された個人暗証番号が含まれており、この番号は二つのキーにより２重に暗号化される。またこのメッセージ中にはカード読取装置３０によつて読み取られた、データ・ベースをアクセスするためのデータも含まれている。要求メッセージ４０はホストＣＰＵ１０へ送られる。

ホストＣＰＵ１０においては、要求メッセージ４０からデータ・ベース１２をアクセスするための番号が抜き出され、データ・ベース１２から認証番号（これは１重に暗号化されたＰＩＮである）

を取り出すのに用いられる。要求メッセージ４０からの２重に暗号化された個人認証番号は、通信キーを用いて復号され、データ・ベースから取り出された、１重に暗号化されたＰＩＮと比較される。両者が等しくなれば、データ・ベース１２からの、１重に暗号化されたＰＩＮは通信キーによつて更に暗号化される。この、結果的に２重に暗号化されたＰＩＮは取引応答メッセージに乗せられて端末装置２０へ送り返され、取引の条件付き承認であることを示す。

端末装置２０は、利用者に鍵盤３２から改めてＰＩＮを入力するよう指示する。取引応答メッセージ４２からの、２重に暗号化されたＰＩＮは２重に復号され、新たに入力されたＰＩＮとの一致性が検査される。そしてもしＰＩＮが一致すれば取引は完了する。

業界への適用の可能性

既述した取引実行システムをこの発明にしたがつて操作すれば、カード・データからの暗号化に

よらず、しかもホストへそのつど通信せずに、利用者から数回にわたる入力によつてＰＩＮの認証が可能になる。これは特に提携銀行間において、ＰＩＮが複数の銀行を通して通信されるさいに、安全な暗号化された形で行なわれるところに価値がある。

4.図面の簡単な説明

第１図は代表的な取引実行システムを表わすブロック図、第２図は第２の代表的な取引実行システムにおける基本的な通信メッセージを示す図、第３図は第１図の取引実行システムにおける基本的な通信メッセージを示す図、第４図は端末装置における取引要求メッセージの発生を示す動作ブロック図、第５図はホストにおける条件付き取引承認メッセージの発生を示す動作流れ図、第６図はホストにおける取引要求メッセージからの暗号化されたＰＩＮ＋ＰＡＤの発生を示す動作ブロック図、第７図はホストにおける条件付き取引承認メッセージのためのデータ・ベースからの暗号化された認証データの発生を示す動作ブロック図、

第８図は取引が拒否された時又は暗号化された比較データが等しい時の取引応答メッセージのフォーマットを示す図、第９図は端末装置における取引応答メッセージに応答したホストへの状況メッセージの発生を示す動作流れ図、第１０図は端末装置における取引応答メッセージで受信された暗号化されたデータからの正当性データの発生を示す動作ブロック図、第１１図は取引が条件付きで承認されたが承認を完了するためには端末装置におけるＰＩＮ検査を必要とする時の取引応答メッセージのフォーマット図である。

１０…Ｂ銀行ＣＰＵ、１２…データ・ベース、１６…Ａ銀行ＣＰＵ、１８…データ・ベース、２０…端末装置、３０…カード読取装置、３２…鍵盤、４６…金融機関テーブル、６０…変数生成機構。

出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション
代理人　弁理士　頓　宮　孝　一
（外１名）

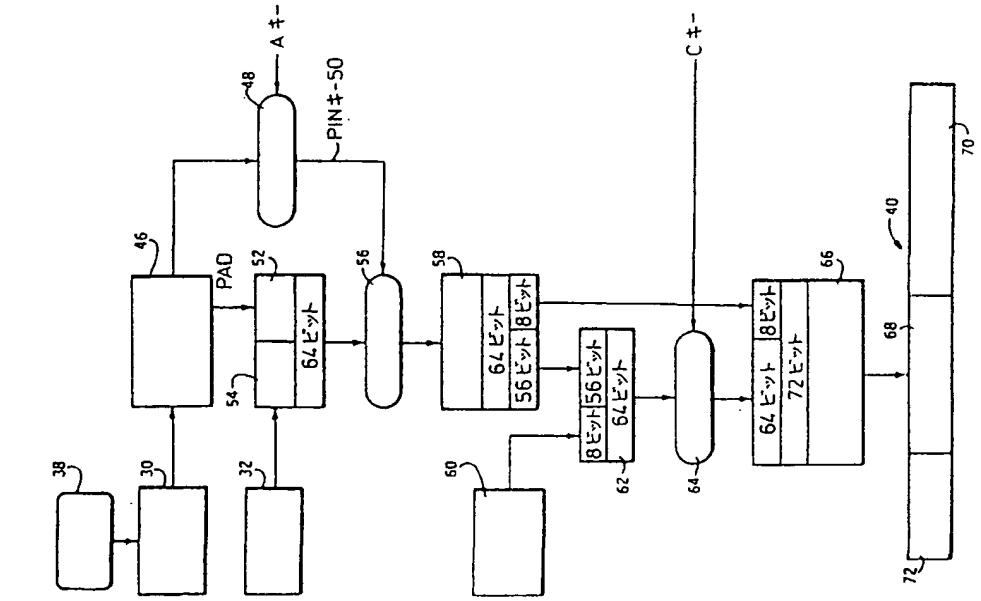

FIG. 4

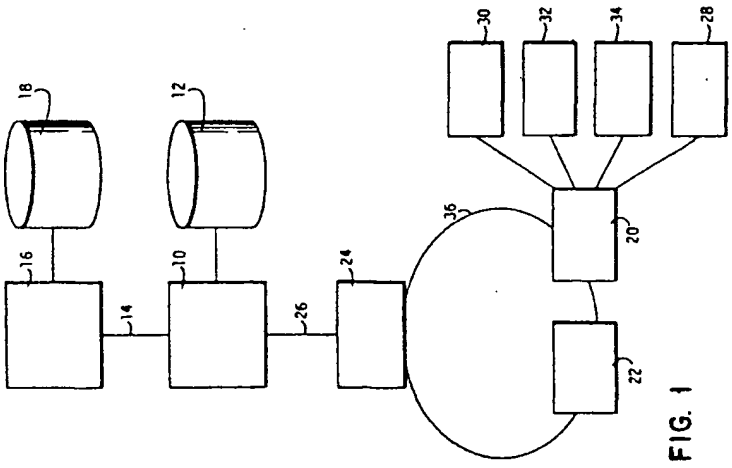

FIG. 1

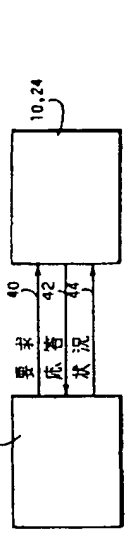

FIG. 2

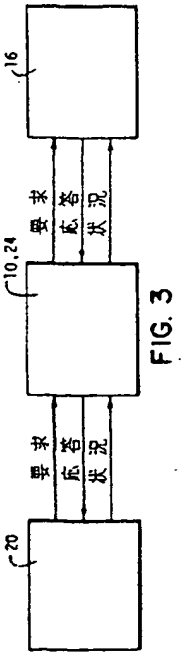

FIG. 3

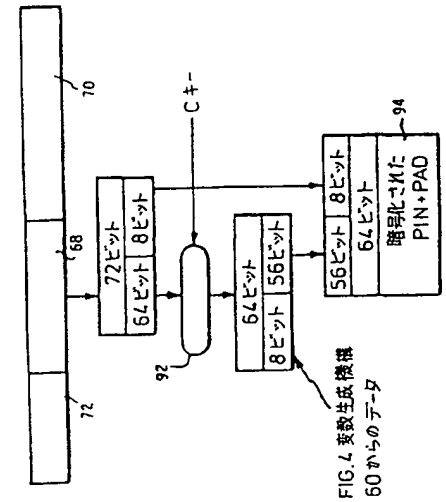

FIG.6

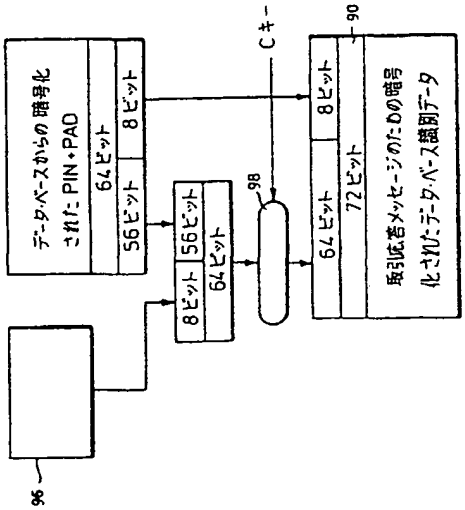

FIG.7

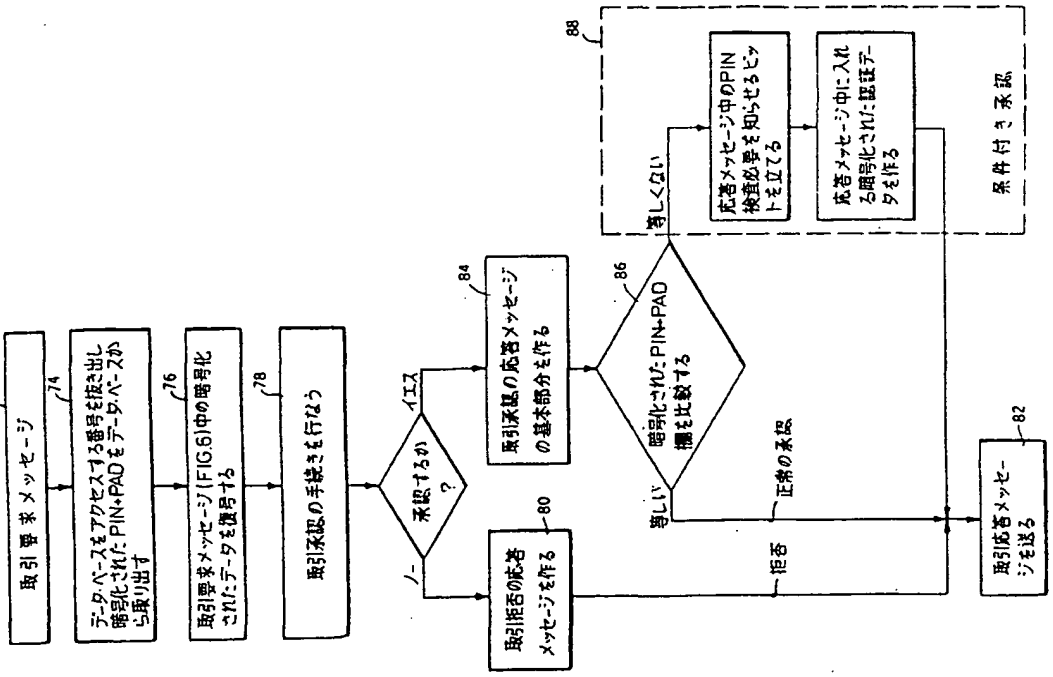

FIG.5

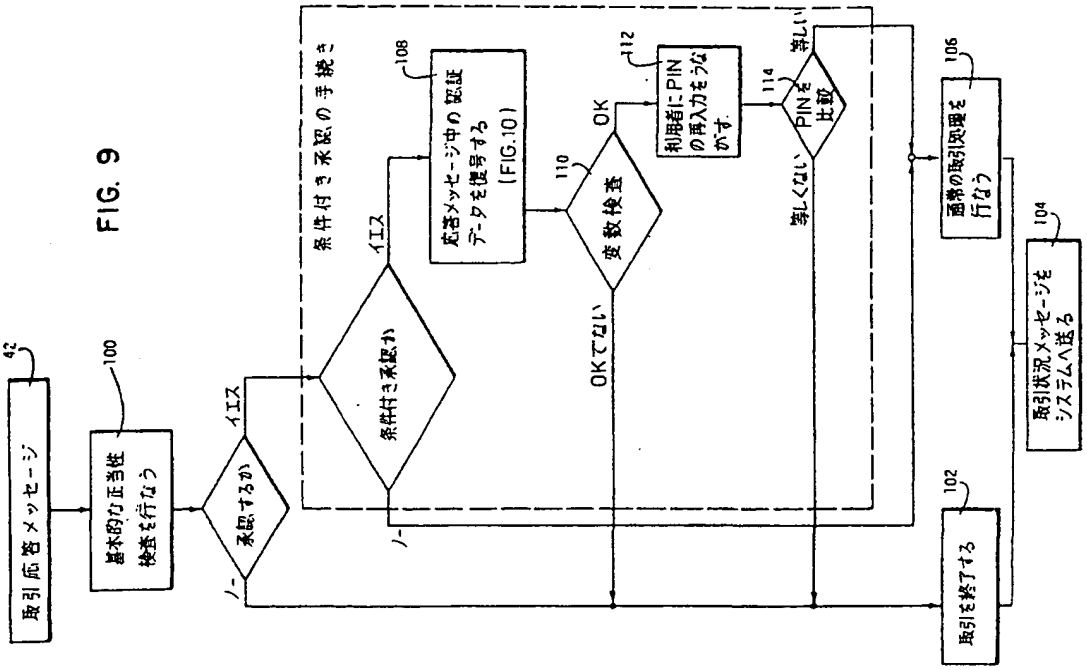

FIG. 9

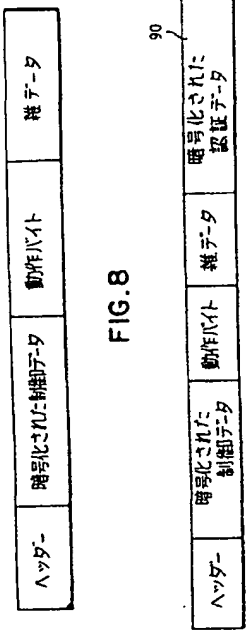

FIG. 8

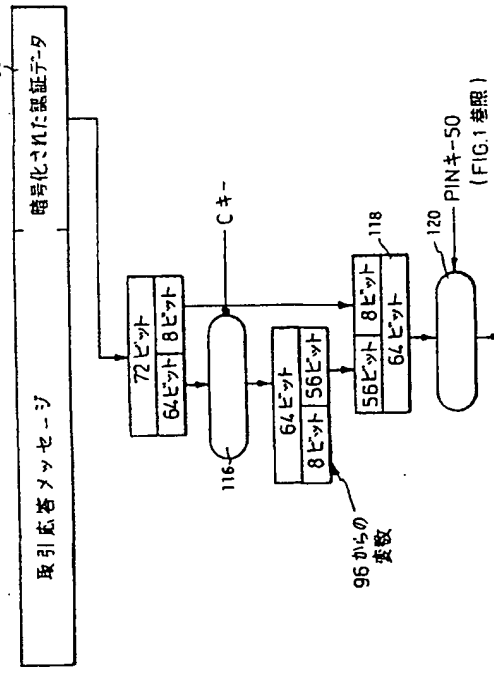

FIG. 11

FIG. 10